eCH-0219 IAM Glossar

Name	IAM Glossar
eCH-Nummer	eCH-0219
Kategorie	Standard
Reifegrad	Definiert; Experimentell; Implementiert; Verbreitet; Auslaufend
Version	0.7
Status	**In Arbeit**
Beschluss am	JJJJ-MM-TT
Ausgabedatum	JJJJ-MM-TT
Ersetzt Version	- <Minor Change; Major Change>
Voraussetzungen	<Vorausgesetzter Standard>
Beilagen	<Beilage>
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Autoren	Annett Laube-Rosenpflanzer, BFH TI, annett.laube@bfh.ch Andreas Spichiger, BFH FBW, andreas.spichiger@bfh.ch Marc Kunz, BFH TI, marc.kunz@bfh.ch Thomas Kessler, Temet, thomas.kessler@temet.ch Adrian Müller, ID Cyber-Identity Ltd, adrian.mueller@cyber-identity.com eCH Fachgruppe IAM
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

Der vorliegende Standard definiert die wichtigsten Begriffe für IAM-Lösungen im föderalen E-Government Schweiz und bildet damit die Grundlage aller eCH Standards im Bereich IAM.

Die aufgenommenen Begriffe umfassen Stakeholder, Prozesse, Services bis zu Implementationsdetails in föderierten und nicht föderierten IAM-Lösungen. Begriffe aus aktuellen internationalen Standards werden zu den definierten Begriffen in Beziehung gesetzt und damit verständlicher gemacht.

Inhaltsverzeichnis

Hinweis

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im vorliegenden Dokument bei der Bezeichnung von Personen ausschliesslich die maskuline Form verwendet. Diese Formulierung schliesst Frauen in ihrer jeweiligen Funktion ausdrücklich mit ein.

1 Einleitung

Internetbasierte Geschäftsprozesse setzen vertrauenswürdige Subjekte und damit verbundenes Wissen um die Handlungspartner voraus. Entsprechende Dienste werden durch die Identitäts- und Zugriffsverwaltung (Identity and Access Management, IAM) gewährleistet. Sie sind beim Bereitstellen von Lösungen im E-Government Schweiz zu berücksichtigen, damit lokale Anwendungen und Dienste sowohl organisationsintern wie auch organisationsübergreifend genutzt werden können. Der Standard definiert die grundlegenden Begriffe und Konzepte im Bereich IAM und dient damit als Grundlage für alle, welche im E-Government-Umfeld Lösungen entwerfen.

1.1 Status

<Zutreffendes fett markieren>

In Arbeit: **Der Gebrauch ist nur innerhalb der Fachgruppe, bzw. im Expertenausschuss zugelassen.**

Entwurf: Das Dokument wurde von den zuständigen Referenten aus dem Expertenausschuss zur öffentlichen Konsultation freigegeben und entsprechend publiziert.

Vorschlag: Das Dokument wird dem Expertenausschuss zur Genehmigung TT-MM-JJJJ vorgelegt, ist aber normativ noch nicht gültig.

Genehmigt: Das Dokument wurde vom Expertenausschuss genehmigt. Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.

Abgelöst: Das Dokument wurde durch eine neue, aktuellere Version ersetzt. Die Benutzung ist zwar noch möglich, es wird aber empfohlen, die neuere Version einzusetzen.

Aufgehoben: Das Dokument wurde von eCH zurückgezogen. Er darf nicht mehr genutzt werden.

1.2 Anwendungsgebiet

Die in diesem Standard definierten Konzepte und Begriffe fassen die Terminologie der bereits bestehenden eCH-Standards im Bereich IAM zusammen und konsolidieren diese. Die aufgenommenen Begriffe umfassen Stakeholder, Prozesse, Services bis zu Implementationsdetails in föderierten und nicht föderierten IAM-Lösungen. Begriffe aus internationalen Standards werden zu den definierten Begriffen in Beziehung gesetzt und damit verständlicher gemacht.

1.3 Anwendungsgebiet

Mit der Schaffung eines Glossars für den Bereich IAM, das mit jedem neuen oder aktualisierten eCH-Standard auf den letzten Stand gebracht wird, wird die Qualität und Konsistenz alles Standards in diesem Bereich erheblich verbessert.

1.4 Schwerpunkt

Kapitel 2 beschreibt die wichtigsten Konzepte und Begriffe auf dem Bereich IAM mit der Einschränkung auf E-Government und E-Health.

1.5 Normativer Charakter der Kapitel

Die Kapitel des vorliegenden Standards sind von normativem oder auch deskriptivem Charakter. definiert die Einordnung der Kapitel.

Kapitel	Beschreibung
1 Einleitung	Deskriptiv
2 Terminologie	Normativ

Anhang A und Anhang C sind ebenfalls normativ. Alle anderen Anhänge dieses Standards sind deskriptiv.

2 Terminologie

2.1 Authentifikator

Der Authentifikator ist das funktionale Abbild des Authentifizierungsmittels der Realwelt. Mit der Funktion eines Authentifikators wird in der Regel aus einem Eingabewert (Challenge) und einem geheimen Wert ein Ausgabewert erzeugt. Je nach Ausprägung muss der geheime Wert durch einen zweiten Faktor (PIN) aktiviert werden.

Synonyme: Authentifizierungsfunktion, engl. Authentificator

2.2 Anbieterin von Zertifizierungsdiensten

Gemäss ZertES [1]: *„Stelle, die im Rahmen einer elektronischen Umgebung Daten bestätigt und zu diesem Zweck digitale Zertifikate ausstellt.“*

Synonyme: Certification Service Provider, Zertifizierungsdienstleistern, Zertifizierungsstelle für digitale Zertifikate,

Überbegriffe: Trust Service Provider (TSP), Vertrauensdiensteanbieter (VDA)

2.3 Attribut / Attribute

Semantisches Abbild einer einem Subjekt zugeordneten Eigenschaft, die das Subjekt näher beschreibt. Der Identifikator ist ebenfalls ein speziell verwendetes Attribut.

Ein Attribut setzt sich zusammen aus den Meta-Attributen Attributname (z.B. „Schuhgrösse“), Attributtyp (z.B. „Integer“) und Attributwert (z.B. „39“).

Im Stellvertretungsfall besitzt die E-Identity des Stellvertreters für eine gewisse Zeit eine

Menge von Attribute der E-Identity des vertretenen Subjekts.

Persönliche Attribute: Attribute die einer natürlichen Person gehören. Dieser alleine muss über die Weitergabe von diesen Attributen entscheiden können.

Enterprise Attribute: Attribute die einer Organisation gehören. Diese entscheidet im Rahmen geltender Gesetze und Verträge über die Weitergabe der Attribute. Der einzelne Benutzer innerhalb der Organisation spielt im Rahmen dieser Entscheidung eine sekundäre Rolle.

2.4 Attribute Assertion Service

Eine Entität, die Attributbestätigungen über eine definierte Schnittstelle ausstellt.

Synonym: Attributbestätigungs Service

2.5 Attribute Service

Der Attribute Service pflegt zeitaktuell ein oder mehrere Attribute für definierte Subjekte.

2.6 Attribut-Autorität (AA)

Eine Attribut-Autorität ist ein Register oder sonstiges Verzeichnis mit einem Attribute Service zur Pflege von Attributen und einem Attribute Assertion Service zur Ausstellung von Attributbestätigungen.

eCH-0167: Informationslieferant, der über eine definierte Schnittstelle (STIAM-Sender) Attribute für die STIAM-Community bereitstellt.

Synonyme: Attribute Authority, Datenlieferant, Informationslieferant

2.7 Attribute-Based Access Control (ABAC)

Konzept dynamischer Zuteilung von Zugriffsrechten basierend auf Attributen des Subjekts.

2.8 Attributaggregation

Der Begriff der Attributaggregation wird von N. Klingenstein in „Attribute Aggregation and Federated Identity“ [2] genau beschrieben. Man versteht darunter den Prozess, Attribute zu einer bekannten digitalen Identität von verschiedenen Quellen abzufragen und zusammenzustellen.

2.9 Attributbestätigung

Bestätigung eines Attributs durch eine Attribut-Autorität. Entspricht einer SAML 2.0 Attribute Assertion [3].

Synonym: Attribute Assertion

2.10 Auditing

a) Überprüfung der Policy-Konformität

b) Aufzeichnung aller Aktionen und Entscheide zur Gewährleistung der Nachvollziehbarkeit

2.11 Authentifizierung

Authentifizierung ist der Vorgang der Überprüfung einer behaupteten E-Identity eines Subjekts nach bestimmten Vorgaben. Das angestrebte Sicherheitsniveau der Authentifizierung bestimmt diese Vorgaben.

Spezialfall eIDAS: dynamische Authentifizierung (kein SSO)

Synonyme: Authentifikation, Authentisierung (todo! Fussnote bemerkung)

2.12 Authentifizierungs-Anfrage

Eine Authentifizierungs-Anfrage wird vom Subjekt an den Authentication Service gesendet. Dieser initialisiert die Überprüfung der behaupteten E-Identity.

Synonym: Authentication Request

2.13 Authentifikation-Autorität (AuthnA)

Eine AuthnA stellt einen Authentication Service zur Verfügung, gegen den sich das Subjekt authentifizieren kann. Der Authentication Service überprüft mittels der Authentifizierungsmittel, die von einem Credential Service ausgestellt werden. Der Credential Service kann ein Bestandteil der AuthnA sein. Beispiele für Authentifikation-Autoritäten sind IdPs (nach SAML), OpenID Provider und MobileID Provider.

Synonym: Authentication Authority

2.14 Authentication Proxy

Ist AuthnA(1) nicht in der Lage, einen Nutzer zu authentifizieren, kann er unter bestimmten Umständen als Authentication Proxy agieren, indem er selber einen eigenen Authentication Request an einen weiteren AuthnA sendet. Die Antwort vom AuthnA(2) kann der AuthnA(1) dann dazu verwenden, eine eigene Response zu generieren.

2.15 Authentication Service

Der Authentication Service überprüft mittels der Authentifizierungsmittel, ob der Zugreifende (Subjekt) der ist, der er behauptet zu sein.

2.16 Authentifizierungsbestätigung

Die Authentifizierungsbestätigung ist der Nachweis, welcher der Identity Provider nach einer erfolgreichen Authentifizierung des Subjektes ausgestellt wird. Die Authentifizierungsbestäti-

gung ist für einen bestimmten Zeitraum gültig und kann eine Vertrauensstufe enthalten.

Beispiele:

Bei Security Assertion Markup Language (SAML) [4] ist die Authentifizierungsbestätigung die „Authentication Assertion“ und wird vom (SAML) Identity Provider ausgestellt.

Bei OIDC [5] ist die Authentifizierungsbestätigung das sogenannte „ID Token“ und wird vom „Authorization Server“ ausgestellt.

Bei Kerberos ist die Authentifizierungsbestätigung ein „Ticket Granting Ticket“ (TGT) und wird vom Kerberos Distribution Center (KDC) ausgestellt.

2.17 Authentifizierungsfaktor

Authentifizierungsfaktoren sind Informationen und/oder Prozesse, die zur Authentifizierung eines Subjektes verwendet werden können. Authentifizierungsfaktoren können auf vier verschiedenen Merkmalen oder auch Kombinationen davon beruhen:

- besitzabhängiger Authentifizierungsfaktor: beruht auf Besitz (etwas, das das Subjekt besitzt, z.B. Zertifikat, Hardware-Token mit privatem Schlüssel, elektronischer Pass oder ID-Karte),

- kenntnisabhängiger Authentifizierungsfaktor: beruht auf Wissen (etwas, das das Subjekt weiss, z.B. Passwort, PIN),

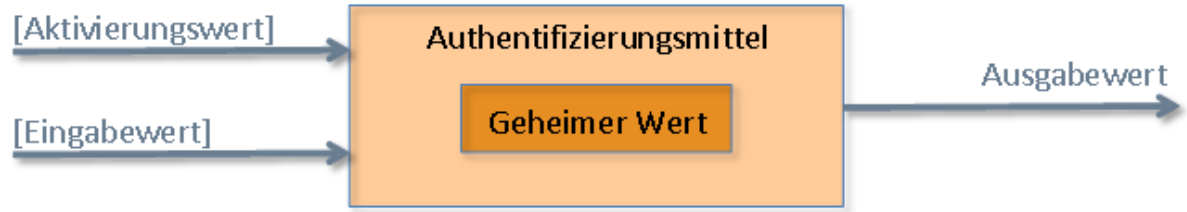
- inhärenter Authentifizierungsfaktor: beruht auf einem biometrischen Merkmal (etwas, das das Subjekt ist, wie Iris, Netzhaut, Fingerabdruck),

- verhaltensbasierter Authentifizierungsfaktor: beruht auf Verhalten (etwas, das welches das Subjekt typischerweise macht, z.B. dynamisches Unterschriftsmuster).

Synonym: Authentifizierungsmerkmal

2.18 Authentifizierungsmittel

Ein Authentifizierungsmittel ist etwas, das ein Subjekt besitzt und das es unter seiner Kontrolle hat (typischerweise ein kryptographischer Schlüssel, ein Geheimnis, ein biometrisches Merkmal oder ein spezifisches Verhalten). Ein Authentifizierungsmittel muss nicht unbedingt in Hardware Form vorliegen, sondern kann auch ein Soft-Token oder eine Software-Komponente sein. Ein Authentifizierungsmittel kann einen (*single-factor authenticator*) oder auch mehrere unabhängige Authentifizierungsfaktoren (*multi-factor authenticator*) benutzen. Der vom Authentifizierungsmittel generierte Ausgabewert (engl. Authenticator output oder authenticator response) wird durch eine mathematische Funktion (Authentifikator oder Authentifizierungsfunktion) aus einem geheimen Wert (z.B. privater Schlüssel), einem oder mehreren optionalen Aktivierungswerten (z.B. PIN oder biometrischer Informationen), und einem oder mehreren optionalen Eingabewerten (z.B. Zufallswerten oder Challenges) generiert. Im Trivialfall kann das Authentifizierungsmittel der geheime Wert selbst sein (z.B. im Fall eines Passworts). Siehe Tabelle 1 für weitere Beispiele.




```
Ausgabewert =
      Authentifizierungsfunktion (geheimer Wert,
                                  [Aktivierungswerte],
                                  [Eingabewerte])
```

Abbildung 1: Schematische Funktionsweise eines Authentifizierungsmittels

	Passwort	Strichliste	SMS	OTP	Mobile-ID	SuisseID
Typ	SFA	SFA	SFA	(HW-)MFA	HW-MFA	HW-MFA
Eingabe-wert	-	Index	gesendeter Code	Seed	gesendeter Code	Nonce
Geheimer Wert	Passwort	(alpha-) numeri-schen Wert	-	Device Key	Private Key	Private Key
Aktivie-rungswert	-	-	-	-	PIN	PIN
Authenti-fikator	-	Liste der (alpha-) numeri-schen Werte	Handy	Device	SIM-Karte	Crypto-Device
Authentifi-zierungs-funktion	Keine oder Hash-Fkt.	Selektion	Lesen und Schreiben des gesen-deten Codes	HMAC	Signatur	Signatur
Ausgabe-wert	Passwort, Hash des Passworts	(alpha-) numeri-schen Wert	gesendeter Code	Code	Sign (ge-sendeter Code)	Sign (Nonce)
Credential[1]	Passwort, Hash des Passworts	Liste der (alpha-) numeri-schen Wer-te	Mobile-Nr.	Device-Nr./ Seed	SIM-Karte mit Mobile-Nr./ Public Key	Certificate

Tabelle 1: Beispiele für Authentifizierungsmittel und zugehörigem Credential

[1] Zum Credential gehört immer auch der Identifier, z.B. der Name des Benutzers.

Synonyme:

- Authenticator (siehe NIST 800-63-3 [6]), früher bei NIST 800-63-2 [7] als Token bezeichnet.
- Bei STORK[2] als identity token bzw. authentication token bezeichnet

2.19 Authorization Service

Der Service überprüft zur Ausführungszeit die Einhaltung der Rechte für die Nutzung der E-Ressource und erlaubt dem Subjekt die Nutzung, wenn es die entsprechenden Rechte besitzt.

2.20 Autorisierung

Administration: Definition der Zugangsregeln und Zugriffsrechte auf eine E-Ressource.

Zur Laufzeit: Prüfen von Zugriffsberechtigung eines authentifizierten Subjektes auf eine Ressource und erteilen des Zugriffs zur Laufzeit. Dabei wird zwischen Grob- und Feinautorisierung unterschieden.

Synonym: Authorization

2.21 Backend Attribute Exchange (BAE)

Attributabfrage im Hintergrund, üblicherweise durch eine Maschine. Ein Benutzer ist bei der Attributabfrage nicht direkt involviert, diese erfolgt ohne seine explizite Zustimmung.

2.22 Behörde

Eine rechtlich begründete Organisation, welche hoheitliche Staatsaufgaben der Schweiz wahrnimmt. Behörden können auf Ebene von Gemeinde, Kanton oder Bund existieren und zur Legislative, Exekutive oder Judikative gehören. (siehe auch eCH-0122[3])

2.23 Benutzerzentriertes Identitätsmanagement

Ermöglicht dem Benutzer die Auswahl spezifischer Authentifizierungsmittel und Attribute zur Bearbeitung in Authentifizierungs- und Attribut-Anfragen und überlässt ihm so die Kontrolle über die eigene, digitale Identität. Das bedeutet nicht, dass der Benutzer jede Transaktion nochmals explizit genehmigen muss, aber dass die Daten immer durch die Identitätsverwaltung des Benutzers fliessen und direkt an seine digitale Identität gebunden sind.

[2] Siehe: https://www.eid-stork2.eu

[3] https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0122&documentVersion=1.0

2.24 Berechtigung

Recht eines Subjekts, bestimmte Ressourcen zu nutzen.

2.25 Bereich STIAM-Domäne

Als Bereich kann eine begrenzte Gruppe von Informationsbezügern und -lieferanten angesehen werden, welche ein bestimmtes Set an Attributen und eine gemeinsame Policy teilen. Die Semantik und Syntax dieser Attribute werden durch die Teilnehmer der Gruppe bestimmt. Beispielsweise soll es möglich sein, dass sich innerhalb von SuisseTrustIAM eine Teilföderation bilden kann, welche nur ihre intern bekannten Identitäten und Attribute über die Plattform austauscht.

2.26 Beweismittel

Ein Beweismittel für die Identitätsüberprüfung ist ein Dokument oder Objekt aus einer verlässlichen Quelle, das Angaben zum Antragsteller enthält.

Ein Beweismittel muss den Namen des Antragsstellers enthalten. Es kann zusätzlich einen eindeutigen Identifikator, körperliche und biometrische Merkmal aber auch beliebige andere Angaben des Antragstellers enthalten. Es sollte Sicherheitsmerkmale enthalten, die ein Reproduzieren erschweren.

Beispiele:

- Beglaubigte Urkunde
- Kreditkarten
- Fahrausweis
- Identitätsdokumente

2.27 Biometrisches Merkmal

Ein biometrisches Merkmal ist ein körperliches Merkmal eines Menschen, das es erlaubt, diesen hinreichend von anderen zu unterscheiden, welches also zu dessen Identifizierung verwendet werden kann. Ein biometrisches Merkmal sollte sich im Laufe der Zeit wenig ändern. Kombinationen mehrere Merkmale sind dabei möglich, z.B. Erfassung des Gesichtes kombiniert mit Stimmerkennung. Ein entscheidender Nachteil bei der Verwendung von biometrischen Merkmalen bei der Authentifizierung ist, dass sie im Fall einer Kompromittierung nicht für ungültig erklärt bzw. neu erzeugt werden können.

Zu den wichtigsten biometrischen Merkmalen gehören:

- Fingerprint
- (dynamische) Unterschrift
- Gesichtsgeometrie
- Gesichtsbild (Foto)

- Irismuster
- Retina (Netzhaut)
- Handgeometrie
- Fingergeometrie
- Ohrform
- Stimme (Klangfarbe)
- DNA
- Geruch
- Tastenanschlag

Zur Identifizierung von natürlichen Personen werden zurzeit meist nur

- Fingerprint
- Iris
- Retina
- Gesichtsgeometrie
- Gesichtsbild (Foto)

verwendet.

Biometrische Merkmale können bezüglich Funktion, Sicherheit, Fälschbarkeit und Anwendungsfreundlichkeit ebenfalls klassifiziert werden. Das NIST hat mit ihrer Online-Dokumentation „Strength of Function for Authenticators – Biometrics“ [8] kurz SOFA-B dazu einen ersten Beitrag geleistet.

2.28 Broker Service

Dieser Service vermittelt zwischen dem Subjekt, Ressourcen und den Services der Ausführungszeit, föderiert Authentifizierung und Attributbestätigung.

2.29 Certification Authority (CA)

Eine Certification Authority ist ein spezieller Credential Service Provider (CSP) als technische Instanz, welche digitale Zertifikate (Public Key Zertifikate, e.g. X.509) als Authentifizierungsmittel ausgibt, erneuert und revoziert. Siehe auch 2.2 Anbieterin von Zertifizierungsdiensten und 2.37 Credential Service Provider (CSP)

Synonyme: Certificate Authority, Certification Service Provider, Trust Service Provider (TSP)

Synonyme deutsch: Zertifizierungsstelle für digitale Zertifikate, Vertrauensdiensteanbieter

2.30 Certificate Policy (CP)

Eine Certifcate Policy enthält die Anwendungsregeln für einen bestimmten Zertifikatstyp.

Siehe auch 2.102 Policy und 2.32 Certification Practice Statement (CPS).

2.31 Certificate Revocation List (CRL)

Liste, welche die von einer (oder mehrere) CA(s) ausgestellten *digitalen Zertifikate* enthält, welche widerrufen wurden. Ein Eintrag in der Liste besteht mindestens aus der Seriennummer des widerrufenen Zertifikats und dem Widerrufsdatum.

2.32 Certification Practice Statement (CPS)

Policy, welche eine Anbieterin von Zertifizierungsdiensten anwendet, um Zertifikate auszustellen. Siehe auch 2.102 Policy und 2.30 Certificate Policy (CP).

2.33 Community Metadaten

Signierter Zusammenzug von Entitätsmetadaten der Mitglieder einer STIAM-Community.

2.34 Client Plattform

Die Client Plattform ist das System oder Gerät, von welchem das Subjekt einen Authentisierungsprozess anstösst. Dies kann beispielsweise ein Browser auf einem PC oder eine Applikation auf einem mobilen Gerät sein.

Synonym: Client, user agent

2.35 Credential

Ein Credential stellt eine Menge von Daten (keine Hardware oder andere physische Container) dar, mit der eine elektronische Identität (E-Identity) an ein Authentifizierungsmittel gebunden wird, welches vom Subjekt besitzt und kontrolliert wird.

Das Credential wird zusammen mit dem Ausgabewert des Authentifizierungsmittel zum Nachweis der behaupteten E-Identity verwendet. Je nach verwendeten Authentifizierungsfaktoren ist das Credential z.B. der Hash eines Passwortes, ein Abbild eines biometrischen Merkmals oder ein Zertifikat (siehe auch Tabelle 1), das zur Definitionszeit von einem CSP an eine E-Identity gebunden wurde.

Ein Credential muss immer auf Authentizität und Vertrauenswürdigkeit überprüft werden, bevor es verwendet wird.

(siehe auch ISO 29115 [9], Annex B und NIST SP 800-63B [10], Kap 3).

Synonym: Identitätsnachweis

2.36 Credential Service

Der Credential Service gibt Authentifizierungsmittel aus und verwaltet sie. Er ermöglicht eine benutzerfreundliche Erneuerung bzw. den Ersatz von Authentifizierungsmitteln. Ein Authentifizierungsmittel bezieht sich auf eine E-Identity und ist auf ein bestimmtes Subjekt ausge-

stellt.

2.37 Credential Service Provider (CSP)

Ein Credential Service Provider ist eine Entität, die als vertrauenswürdiger Herausgeber von digitale Zertifikaten und anderer Sicherheits-Tokens (Authentifizierungsmitteln) agiert.

Der CSP kann eine eigene Registration Authorities (RA) enthalten und Dienste zur Verifizierung der Credentials (Identity Provider) umfassen. Ein CSP kann als öffentliche Instanz auftreten, oder als Dienst in eine abgeschlossene Domäne integriert sein.

2.38 Definitionszeit

In der Definitionszeit wird das IAM-System eingerichtet und konfiguriert. Zusätzlich werden die elektronischen Identitäten etabliert. Die Definitionszeit umfasst damit die Prozesse zur Bereitstellung aller notwendigen Informationen für alle beteiligten Komponenten sowie der Komponenten selbst.

2.39 Dienstanbieter

Der Dienstanbieter ist ein Stakeholder in einem IAM-System, der einen oder auch mehrere (IAM-)Dienste zur Verfügungen stellt, die es dem Leistungsbezüger ermöglicht auf Leistungen zuzugreifen und gleichzeitig diese zu schützen.

2.40 Digitales Zertifikat

Strukturierte Daten, die den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels bestätigen.

Synonym: Digital Certificate, Zertifikat, Public-Key-Zertifikat

2.41 Ding

Ein Ding ist ein physischer Gegenstand, welcher über ein Netzwerk erreichbar ist. Innerhalb des Netzwerkes ist das Ding mit einem Identifikator identifizierbar. Mehrere Dinge, welche im selben Netzwerk verknüpft sind, bilden ein Internet der Dinge (Internet of Things IoT).

Synonyme: Objekt, Thing (IoT)

2.42 Discovery Service (WAYF - Where Are You From)

Der Discovery Service ist dafür zuständig, den Benutzer zu einem Identity Provider seiner Wahl zwecks Authentifizierung zu leiten.

2.43 Domäne

Administrative / technische Gemeinschaft oder Organisation mit einer gemeinsamen Policy.

2.44 E-Identity

Eine E-Identity ist die Repräsentation eines Subjekts. Eine E-Identity (digitale Identität) hat einen Identifikator (eindeutiger Name), meist zusammen mit einer Menge von zusätzlichen Attributen, welche innerhalb eines Namensraumes eindeutig einem Subjekt zugewiesen werden können. Ein Subjekt kann mehrere E-Identities haben.

Eine notifzierte E-Identity ist eine E-Identity, die alle in eIDAS 910/2014 [11] Artikel 7 aufgeführten Voraussetzungen erfüllen muss.

Synonyme: Digitale Identität, Digital Identity, Elektronische Identität, Electronic Identity

2.45 E-Identity Service

Der E-Identity Service stellt zu Subjekten E-Identities aus und verwaltet sie.

2.46 E-Ressource

Digitale Repräsentation einer Ressource. Eine E-Ressource hat einen Identifikator (eindeutiger Name, oft URL/URI), welcher innerhalb eines Namensraumes eindeutig einer Ressource zugewiesen werden kann. Eine Ressource kann mehrere E-Ressourcen haben.

2.47 E-Ressource Service

Der E-Ressource Service stellt zu Ressourcen E-Ressourcen aus und verwaltet sie.

2.48 Eigenschaften

Eigenschaften sind charakteristische Merkmale oder charakteristische Verhalten eines Subjekts, die in ihrer Summe spezifisch für das Subjekt sind.

2.49 Entität

Ein aktives Element eines IT Systems, z.B. ein automatisierter Prozess oder eine Menge von Prozessen, ein Teilsystem, eine Person oder eine Gruppe von Personen mit definierten Funktionalitäten [3].

Organisation mit definierter Rolle innerhalb einer STIAM-Community.

Synonym: Entity

2.50 Elektronische Signatur

Gemäss ZertES [1]: *„Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder die logisch mit ihnen verknüpft sind und zu deren Authentifizierung dienen.“*

2.51 Elektronisches Identifizierungsmittel

Begriff aus eIDAS 910/2014 [11]: „Elektronisches Identifizierungsmittel“ ist eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird.

Ein elektronisches Identifizierungsmittel enthält Authentifizierungsfaktoren, Attribute für Personen und hat eine Gültigkeit. Bei einer (dynamischen) Authentifizierung wird der gesamte Prozess Subjekt authentifizieren vom elektronischen Identifizierungsmittel abgewickelt. Es umschliesst daher sowohl Authentifizierungsmittel, Credential und IdP. Das Ergebnis einer Authentifizierung mit einem elektronischen Identifizierungsmittel ist eine Authentifizierungsbestätigung, mit der die Identität des Subjekts und die erfolgreiche Authentifizierung bestätigt werden.

Beispiele für elektronische Identifizierungsmittel sind der neue deutsche Personalausweis (nPA) inkl. Middleware (AusweisApp) oder die gesamte SuisseID Infrastruktur bestehend aus SuisseID Token, Middleware (Gerätetreiber) und SuisseID IdP.

2.52 Elektronisches Identifizierungssystem

Begriff aus eIDAS 910/2014 [11]: „Elektronisches Identifizierungssystem“ ist ein System für die elektronische Identifizierung, in dessen Rahmen natürlichen oder juristischen Personen oder natürlichen Personen, die juristische Personen vertreten, elektronische Identifizierungsmittel ausgestellt werden.

Ein notifiziertes elektronisches Identifizierungssystem muss alle in eIDAS 910/2014 [11] Artikel 7 aufgeführten Voraussetzungen erfüllen.

2.53 Elektronisches Siegel

Eine *elektronische Signatur*, welche im Namen einer *UID-Einheit* angebracht wird. Elektronische Siegel können im Rahmen automatisierter Prozesse erstellt werden.

2.54 Empfängerbaustein

Der Empfängerbaustein realisiert eine standardisierte STIAM-Schnittstelle für eine Relying Party, welche die STIAM-Protokolle nicht direkt unterstützt (vgl. 2.132 STIAM-Komponente Abbildung 3: STIAM-KomponentenAbbildung 3).

2.55 Entitätsmetadaten

Metadaten einer Attribut-Autorität oder Relying Party zur Definition der Rolle einer Entität innerhalb der STIAM-Community.

2.56 Feinautorisierung

Gewährung bzw. Verweigerung des Zugriffs auf einzelne von einer Ressource bereitgestell-

ten Funktionen oder Daten.

2.57 Föderiertes IAM-System

Eine Identitäts-Föderierung ist eine Zusammenarbeit verschiedener Entitäten eines IAM-Systems über Organisations- und Systemgrenzen hinweg, ohne Duplikation oder Replikation der dazu notwendigen Benutzerdaten (E-Identities und Attribute) im Gegensatz zum replizierenden IAM-System (siehe 2.112 Replizierendes IAM-System).

Eine Föderierung von Identitäten erlaubt es, Informationen über eine Authentifizierung eines Subjektes und optional Identitätsinformationen zu diesem Subjekt über ein Netzwerk zu übermitteln.

Damit ein föderiertes IAM-System etabliert werden kann, müssen sich die verschiedenen Domänen in Bezug auf bestimmte Aspekte gegenseitig vertrauen. Dieses Vertrauen stützt sich auf explizite und implizite Vereinbarungen ab.

Wie in Abbildung 2 dargestellt besteht ein föderiertes Identitätssystem aus den drei Entitäten Subjekt, Relying Party (RP) und einem Identity Provider (IdP). Je nach Ausprägung des verwendeten Protokolls ist die Abfolge der Informationen anders. Das Subjekt kommuniziert dabei aber immer mit dem IdP, wie auch mit der RP. Das Subjekt authentisiert sich gegenüber dem IdP in einem primären Authentisierungsverfahren mit einem bestimmten Authentifizierungsmittel (Authenticator). Dieses Ereignis wird dann in Form einer Authentifizierungsbestätigung an die vertrauende Partei über das Netzwerk weitergegeben. Der IdP kann zu dieser Authentifizierungsbestätigung noch weitere (Personen-)Attribute zum authentisierten Subjekt beifügen.

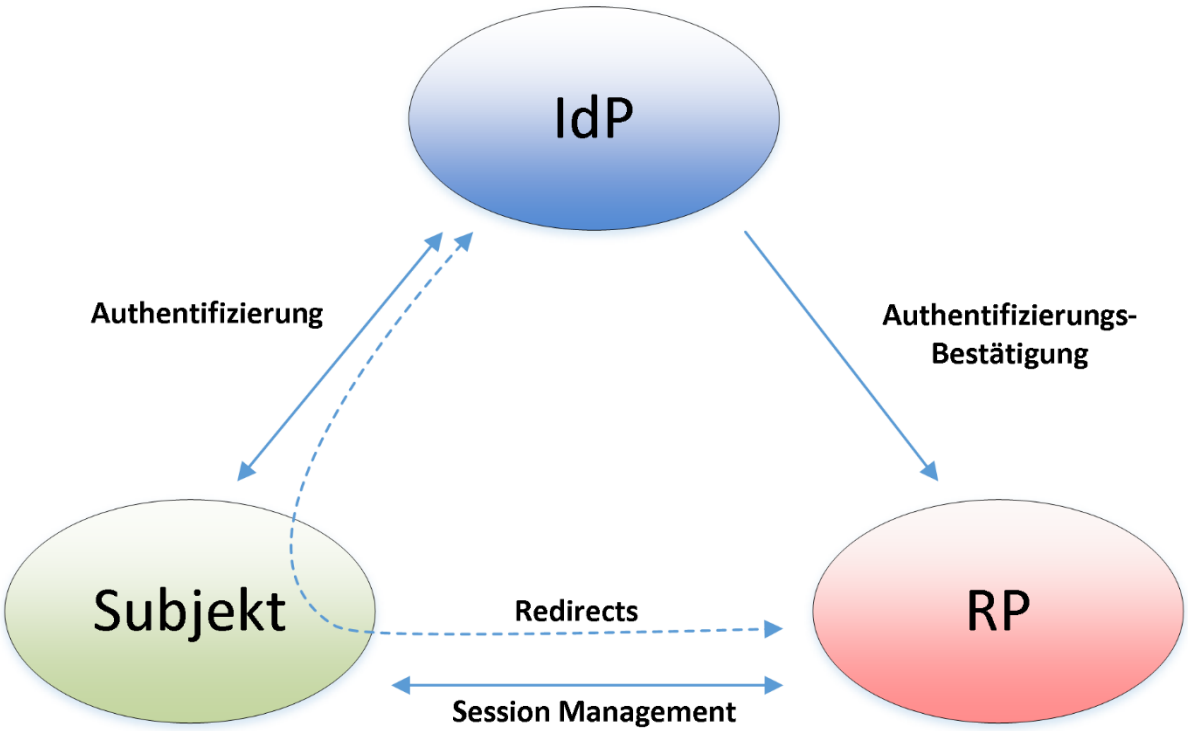


Abbildung 2: Modell einer Identity Federation

Föderiertes IAM-System im E-Government: Beim föderierten IAM-System im E-

Government stellen Behörden (siehe 2.22) Ressourcen den Subjekten ihren internen (andere Behörden der Schweiz) oder externen Partnern (Personen, Unternehmen, Organisationen oder Behörden anderer Staaten) zur Verfügung, mit denen definierte Leistungen aus dem Bereich ihrer Zuständigkeit online verfügbar gemacht werden. Diese Ressourcen sollen für Subjekte der eigenen Domäne(n) und für Subjekte mit E-Identities anderer Domänen zugreifbar sein. Eine Behörde kann somit Relying Party (siehe 2.111 Relying Party (RP)) aber auch u.U. gleichzeitig IAM-Dienstanbieter (siehe 2.63 IAM-Dienstanbieter) sein.

Synonyme: Federation, Föderierung, föderiertes Identitätssystem, föderiertes IAM-System

2.58 Führung

Die Führung ist ein Stakeholder in einem IAM-System, die Leistungserbringer und Dienstanbieter koordiniert, um das IAM-System zu implementieren und zu regelkonform betreiben.

2.59 Funktion

Eigenschaft, die einem Subjekt bestimmte Aufgaben, Kompetenzen und Verantwortung innerhalb einer Organisation zuweist. Ein Subjekt kann mehrere Funktionen haben (vgl. Rolle).

2.60 Geregeltes Zertifikat

Ein auf eine *natürliche Person* oder eine *UID-Einheit* ausgestelltes *digitales Zertifikat*, welches die entsprechenden Formvorschriften des ZertES [1] erfüllt. Geregelte Zertifikate können z.B. für elektronische Siegel oder zur Website-Authentisierung eingesetzt werden.

2.61 Grobautorisierung

Gewährung bzw. Verweigerung des Zugangs zu einer Ressource.

2.62 Globally Unique Identifier (GUID)

Ein Globally Unique Identifier ist eine eindeutige Nummerierung und kann zu einem Subjekt zugeordnet werden.

2.63 IAM-Dienstanbieter

Die Rolle IAM-Dienstanbieter beschreibt Betreiber von einem oder mehreren IAM-Geschäftsservices gemäss Kapitel „2.65 IAM-Geschäftsservices“. Es werden die folgenden Entitäten unterschieden, die aber oft gemeinsam implementiert werden.

- 2.109 Registrierungsstelle
- 2.37 Credential Service Provider (CSP)
- 2.75 Identity Provider (IdP)
- 2.6 Attribut-Autorität (AA)

- 2.142 Vermittler

2.64 IAM-Führung

Die Rolle IAM-Führung ist verantwortlich für das Managen der IAM Dienstanbietern (siehe 2.63 IAM-Dienstanbieter) und der Relying Parties (siehe 2.111 Relying Party (RP)) analog ITIL oder IT4IT in allen Fachbereichen wie z.B. Release-Management, Qualitätsmanagement, IAM-Lieferanten- und -Konsumentenmanagement, Inzident-, Event-, Service-Request-Management. Dies kann sowohl im internen Kontext als auch über Verträge/SLA mit externen IAM-Dienstanbietern und -Konsumenten geschehen.

2.65 IAM-Geschäftsservices

Die Geschäftsservices erbringen ihre Aufgaben mit Hilfe von IT. Dabei arbeiten sie über standardisierte Schnittstellen zusammen, welche offene Standards (z.B. SAML, OIDC, …) benutzen. Jeder IAM-Geschäftsservice wird von einem IAM-Dienstanbieter erbracht. Die Nutzung ist vertraglich geregelt. Geschäftsservices sind keine technische Service-Komponenten, d.h. bei einer Realisierung können ein oder auch mehrere Geschäftsservices von einer technischen Service-Komponente implementiert oder auch ein Geschäftsservice auf mehrere technischen Service-Komponenten verteilt werden.

2.66 IAM-Policy

Die IAM Policy definiert die Ziele, Prinzipien und die Systemgrenzen des angestrebten IAM-Systems.

2.67 IAM-Regulator

Die Rolle IAM-Regulator (oder IAM-Steuerung) definiert die rechtlichen, prozessualen, organisatorischen und technischen Rahmenbedingungen, innerhalb derer das IAM abgewickelt werden kann. Der IAM-Regulator beteiligt alle anderen Rollen in geeigneter Weise an der Definition.

IAM-Regulatoren existieren in verschiedenen Formen und können sowohl innerhalb einer einzigen Organisation, aber auch organisationsübergreifend agieren.

Die **Steuerung** definiert die IAM-Policy für ein organisationsinternes oder -externes IAM-System bzw. von IAM-Geschäftsservices.

Der **Gesetzgeber** definiert die rechtlichen Rahmenbedingungen.

Das **Standardisierungsgremium** erstellt Normen und Richtlinien für die prozessualen, organisatorischen und technischen Rahmenbedingungen.

2.68 IAM-Support

Die Rolle IAM-Support ist verantwortlich für alle Aktivitäten zum Auffinden und Lösen von Problemen, die zur Lauf- oder Definitionszeit auftreten können.

2.69 Identifikator

Eine Zeichenkette, welche eine E-Identity oder eine E-Ressource innerhalb eines Namensraumes (Domäne) eindeutig bezeichnet. Der Identifikator einer Ressource ist oft eine URL/URI.

2.70 Identifizierung

Identifizierung ist ein Vorgang zur Definitionszeit, bei welchem die Identität des Subjekts meist mit Hilfe von Beweismitteln überprüft wird. Die Identifizierung wird meist durch eine Registrierungsstelle als Teil der Registrierung durchgeführt.

Synonym: Identitätsfeststellung

2.71 Identität

Identität ist die Gesamtheit der ein Subjekt kennzeichnenden und als Individuum von allen anderen unterscheidenden Eigentümlichkeiten. Im IAM-Kontext wird hauptsächlich die E-Identity eines Subjekts verwendet (siehe 2.44 E-Identity).

Synonym: Identity

2.72 Identitäts- und Zugriffsverwaltung / Identity und Access Management (IAM)

Alle Prozesse und Systeme um Subjekten den Zugriff auf die Ressourcen zu ermöglichen, die diese auf Grund ihrer Funktion in der Organisation benötigen.

Synonym: Identity und Access Management (IAM)

2.73 Identitätsdokument

In der Schweiz gelten die folgenden Dokumente als Identitätsdokumente:

- Reisepass,
- Schweizer Identitätskarte,
- eine für die Einreise in die Schweiz anerkannte Identitätskarte.

2.74 Identity Linking

Identity Linking ist der Vorgang, bei welchem eine LinkedID an eine eindeutige, digitale Identität eines Subjekts geknüpft wird. Die dazu notwendigen Informationen werden in einer Link Table abgelegt.

2.75 Identity Provider (IdP)

Entität, die E-Identity verwaltet und herausgibt. Ein IdP stellt einen Authentication Service

und meist auch einen Attribute Assertion Service zur Verfügung.

Synonym: Authorization Provider

2.76 Identity Provider/ Attribut-Autorität (IdP/AA)

Im SuisseTrustIAM-Kontext können Unternehmen und Organisationen als Informationslieferanten eine IdP/AA-Komponente bereitstellen, welche als IdP agiert, aber auch zu einer ihr bekannten Identität Informationen in Form von Attributen ausstellen kann. (vgl. auch 2.131 STIAM-IdP, 2.136 STIAM-Sender und 2.132 STIAM-Komponente Abbildung 3).

Konzeptionell ist eine IdP/AA-Komponenten ein Mini-Vermittler (siehe 0), an dem ein IdP und die dazugehörige AA angeschlossen sind. Dieser Vermittler liefert als Antwort auf eine Authentifizierungsanfrage zusätzlich zu einer Authentifizierungsbestätigung auch Attributbestätigungen.

2.77 Juristische Person

Juristische Personen sind Organisationen nach Art. 52 ff ZGB sowie gemäss den einschlägigen Bestimmungen des Gesellschaftsrechtes des OR definiert.

Juristische Personen können nur durch natürliche Personen handeln und sind daher immer an eine natürliche Person gebunden (vgl.2.137 Subjekt).

2.78 Körperliches Merkmal

Ein körperliches Merkmal ist ein Merkmal eines Menschen, wie Körpergrösse und Augenfarbe. Spezielle körperliche Merkmale sind die biometrischen Merkmale (siehe 2.27 Biometrisches Merkmal).

2.79 Kryptographischer Token

Software- oder Hardwaremedium zur Speicherung des/der privaten Schlüssel eines Zertifikates (Bsp. f. Software: Microsoft Certificate Manager im Windows OS; Bsp. f. Hardware: SmartCard, USB-Token, Hardware Security Module)

Synonym: Zertifikatstoken, Cryptographic Token, Kryptografischer Token

2.80 Laufzeit

Zur Laufzeit finden die elektronischen Prozesse statt, mit denen ein Subjekt – im Erfolgsfall – Zugang und Zugriff auf die Ressourcen einer Relying Party erhält.

Synonym: Ausführungszeit

2.81 Leistungsbezüger (LB)

Der Leistungsbezüger ist ein Stakeholder in einem IAM-System, der eine fachliche Leistung in Anspruch nehmen möchte, die in Form einer Ressource von einem Leistungserbringer zur

Verfügung gestellt wird. Dazu muss der Leistungsbezüger Dienste für die Authentifizierung und Autorisierung verwenden, die von Dienstanbietern zur Verfügung gestellt werden.

2.82 Leistungserbringer (LE)

Der Leistungserbringer ist ein Stakeholder in einem IAM-System, Ressourcen zur Verfügung stellt, die von Leistungsbezügern verwendet werden. Zum Schutz der Ressourcen nimmt er gemäss seinen Bedürfnissen (z.B. Risikobereitschaft, Wirtschaftlichkeit) Dienste der Dienstanbieter in Anspruch.

2.83 LinkedID

Im organisationsübergreifenden Kontext erlaubt LinkedID, E-Identities aus verschiedenen Domänen miteinander in Beziehung zu setzen. E-Identities können mit LinkedIDs zu einem beliebigen gerichteten Graphen verkettet werden.

2.84 Linking Protokoll

Der Benutzer kann IdPs oder AAs in der Link Table seines Accounts verbinden. Um den korrekten Identifikator als Eintrag in der Link Table zu erhalten, muss sich der Benutzer gegenüber dem jeweiligen Authentication Service authentisieren. Dadurch kann ein eindeutiger Identifikator zwischen STIAM-Hub und dem IdP oder der AA ausgetauscht werden.

2.85 Logging Service

Der Logging Service dokumentiert zur Ausführungszeit die Verwendung eines Services und stellt der Support-Organisation die notwendigen Informationen bereit, um Nutzungsprobleme oder Fehler aufzuklären.

2.86 Look-Up Secrets

Look-Up Secrets enthalten eine Liste von (alpha-)numerischen Werten, die zuvor zwischen dem Subjekt und dem Credential Service Provider (CSP) ausgetauscht wurden. Zur Authentifizierung muss der Benutzer einen bestimmten Wert aus dieser Liste angegeben.

Die ausgetauschten Werte müssen zufällig generiert werden. Sie dürfen nur einmal benutzt werden und eine genügend hohe Entropie besitzen.

Beispiele: Strichlisten (engl. tally sheet) oder TAN-Blöcke

Synonym: Nachschlagbares Geheimnis

2.87 Memorized Secrets

Memorized Secrets, im Allgemeinen als Passwort oder PIN bezeichnen, sind geheim gehaltene Werte, die meist vom Benutzer gewählt und in seinem Gedächnis oder an einem anderen sicheren Aufbewahrungsort gespeichert werden. Sie müssen über eine genügend hohe Komplexität und Zufälligkeit verfügen, um von einem Angreifer nicht erraten oder auf sonsti-

ge Art und Weise berechnet werden können. Passwort Policies legen die Regeln zur Länge, Komplexität, Zeichenmix, Ablaufdauer und Wiederverwendung fest und bestimmen somit die Stärke des Memorized Secrets.

Beispiele: Passwort oder PIN

Synonym: gespeichertes Geheimnis

2.88 Meta-Attribut

Bestandteil des Attribut-Schemas, Spezifizierung des Attributs.

2.89 Metadaten

Ein Mittel, um Vertrauen und technische Interoperabilität zwischen SAML Komponenten (Entitäten) zu ermöglichen. Können auch verwendet werden, um Attributinformationen auszutauschen.

Die Metadaten beschreiben die Komponenten der registrierten Organisationen und Provider mit ihren Federation-Service-Endpunkten, Zertifikaten und den angeforderten bzw. zur Verfügung gestellten Attributen.

Synonym: Metadata

2.90 Meta-Domäne

Domäne, welche die Zusammenarbeit zwischen zwei oder mehreren Domänen regelt.

2.91 Multi-Factor Cryptographic Devices

Ein multi-factor cryptographic device ist ein physisches Gerät, welches einen geschützten kryptographischen Schlüssel enthält. Es muss mit einem zweiten Authentifizierungsfaktor (Wissen oder Eigenschaft) aktiviert werden. Die Authentifizierung wird durch den Besitznachweis und Kontrolle des kryptographischen Schlüssels vollbracht.

Beispiele: SmartCard, SuisseID

Synonym: Multifaktor Verschlüsselungs-Geräte

2.92 Multi-Factor Cryptographic Software

Ein multi-factor software cryptographic authenticator ist ein kryptographischer Schlüssel, welcher auf einer Festplatte oder ähnlichem Medium gespeichert ist. Ein solcher Authenticator muss mit einem zweiten Authentifizierungsfaktor aktiviert werden. Die Authentifizierung wird durch den Besitznachweis und Kontrolle des kryptographischen Schlüssels vollbracht. Dieser Authenticator kombiniert 2 Authentifizierungsfaktoren: Besitz (kryptographischer Schlüssel) mit einem weiteren Geheimnis (Besitz oder Eigenschaft), das zur Aktivierung verwendet wird.

Beispiel: Soft-Token (PKCS#12 Datei)

Detaillierte Anforderungen sind in den folgenden Quellen beschrieben:
Siehe auch NIST SP 800-63B [10], Kapitel 5.1.7.

Synonym: Multifaktor Verschlüsselungs-Software

2.93 Namensraum

Anwendungsbereich (z.B. ein Unternehmen, ein Staat, eine Fachgemeinschaft, eine Sprachgemeinschaft), für welchen die Bedeutung einer Zeichenkette (z.B. Identifikator) definiert ist.

Synonym: Namespace

2.94 Natürliche Person

Eine natürliche Person ist ein Mensch als Rechtssubjekt.

Synonyme: Benutzer, User

2.95 Netzwerk

Informationssystem welches in der Lage ist, Informationen mit verschiedenen verbundenen Komponenten auszutauschen.

2.96 Nichtabstreitbarkeit

Die Garantie bzw. der Beweis, dass sich ein Subjekt auf die Korrektheit der Daten bzw. den Inhalt eines elektronischen Dokuments verpflichtet hat. Nicht-Abstreitbarkeit ist ein wichtiger Bestandteil der qualifizierten elektronischen Signatur.

Synonyme: Non-Repudiation, Content-Commitment

2.97 Online Certificate Status Protocol (OCSP)

Bei OCSP handelt es sich um ein Protokoll zur Abfrage des Gültigkeitsstatus eines digitalen Zertifikats. Siehe auch 2.147 Widerruf und 2.31 Certificate Revocation List (CRL).

2.98 OpenID Connect

OpenID Connect 1.0 (OIDC) [5]definiert eine einfache Identitätsschicht auf der Basis von OAuth 2.0 (RFC 6749) [12], die auch von Mobilgeräten verwendet werden kann. OIDC verwendet das Basisprotokoll OAuth sowohl für die Authentifizierung als auch für die Zugangskontrolle. Als Security-Tokens werden JSON Web Tokens [13] verwendet.

2.99 Organisation

Eine Organisation ist eine Gruppe aus mehreren natürlichen oder juristischen Personen (Unternehmen, Verein, Amtsstelle, Gruppe von Subjekten). Eine Organisation kann

(Unter-)Organisationen enthalten.

Bei Organisationen wird zwischen handelnden und nicht handelnden Organisationen unterschieden. Handelnde Organisationen, z.B. Gruppen-Accounts, können sich authentifizieren und Zugriff zu Ressourcen erhalten. Nicht handelnde Organisationen, wie z.B. juristische Personen, können sich nicht selbst authentifizieren, sondern nur über die dazugehörige natürliche Person.

2.100 OTP Devices

Ein Single-Factor OTP Device ist eine Software oder ein Gerät, welches nach einem bestimmten Algorithmus (pro Ereignis, Zeitbasiert) spontan ein Einmal-Passwort generiert.

Auf dem Gerät oder in der Applikation befindet sich ein eingebettetes Geheimnis (Schlüssel), welches für die Generierung des einmal verwendbaren Passwortes genutzt wird. Als Eingabewert kann die aktuelle Zeit oder ein sich inkrementierender Zähler dienen.

Beispiele: SecureID-Token, Google Authenticator, SafeNet mobilePass

Ein Multi-Factor OTP Device erfordert zur Aktivierung des Algorithmus einen zweiten Faktor (Wissen oder Eigenschaft) auf dem Gerät. Dieser zweite Authentifizierungsfaktor kann ein integriertes Keypad, ein biometrischer Sensor (z.B. Fingerabdruck) oder eine direkte Computer Schnittstelle (z.B. USB) sein.

Beispiele: SecureID-Token mit Keypad, HID ActivID Token

Synonym: Einmal-Passwort Generator

2.101 Out of Band Authenticators

Out of Band ist ein physisches Gerät, welches eindeutig adressierbar sein muss und welches Geheimnisse die vom CSP gewählt werden, zur einmaligen Verwendung empfangen kann.

Das Gerät ist im Besitz des Subjekts und sollte über einen eigenen, privaten Kanal angesprochen werden können, welcher unabhängig vom primären Kanal für den zweiten Authentifizierungsfaktor genutzt wird.

Der Out of Band Authenticator kann auf 2 verschiedene Arten funktionieren:

1. Das Subjekt präsentiert das Geheimnis, welches er über den zweiten Kanal erhalten hat dem authentifizierenden Dienst über den primären Kommunikationskanal.
2. Das Subjekt sendet dem authentifizierenden Dienst eine Antwort direkt über den zweiten Kommunikationskanal zurück.

Beispiele: Handy/Smartphone mit Mobilnummer und SMS-TAN-Verfahren

Synonym: Externer Kanal

2.102 Policy

Schriftlich festgehaltene Regelungen und Vorschriften, welche einzuhalten sind.

2.103 Qualifizierte elektronischen Signatur

Eine elektronische Signatur, welche die entsprechenden Formvorschriften des ZertES [1] erfüllt. Eine qualifizierte elektronische Signatur kann als Pendant der eigenhändigen Unterschrift in der elektronischen Welt betrachtet werden.

2.104 Qualifiziertes Zertifikat

Ein auf eine *natürliche Person* ausgestelltes *digitales Zertifikat*, welches die entsprechenden Formvorschriften des ZertES [1] erfüllt. Eine *qualifizierte elektronische Signatur* muss auf einem qualifizierten Zertifikat beruhen.

(Anmerkung: In der EU-Verordnung eIDAS 910/2014 [11] ist die Definition des qualifizierten Zertifikats weiter gefasst. Dort umfasst dieser Begriff neben dem Zertifikat für qualifizierte elektronische Signatur auch Zertifikate für elektronische Siegel und für Website-Authentifizierung. Siehe dazu auch *geregelten Zertifikat*.)

2.105 Quality Authentication Assurance (QAA)

Qualität der Authentifikation einer digitalen Identität gemäss ISO 29115:2013 [9].

2.106 Rechte

Die Rechte sind spezifische abstrakte Eigenschaften, welche das Subjekt besitzen muss, um auf eine Ressource zugreifen zu dürfen. Diese können z.B. in Gesetzen oder Verträgen festgelegt sein.

2.107 Register

Verzeichnisse in der Verwaltungssprache, wie z.B. die Einwohnerregister, Anwaltsregister, Zivilstandsregister, Handelsregister etc. Sie werden in der Regel von offiziellen Stellen (Verwaltungen, Behörden) geführt.

2.108 Registrierung

Prozess einer Registrierungsstelle, bei dem ein Subjekt eine E-Identity mit dazugehörigem Authentifizierungsmittel und Credential erlangt. Die Registrierung beinhaltet meist eine *Identifizierung*.

Synonym: Registration

2.109 Registrierungsstelle (RA)

Eine Registrierungsstelle ist eine Entität, die genügend Informationen zu einem Subjekt erfasst und überprüft, um dessen Identität überprüfen zu können.

Die RA kann ein integraler Bestandteil eines CSP sein oder als eigener Dienst im Auftrag des CSP handeln.

Synonym: Registration Authority

2.110 Regulator

Der Regulator ist ein Stakeholder in einem IAM-System, der durch die Definition der rechtlichen, prozessualen, organisatorischen und technischen Rahmenbedingungen für das IAM-System, die Interoperabilität, Robustheit und Sicherheit sicherstellen möchte.

2.111 Relying Party (RP)

Die Relying Party vertritt die Interessen der Ressource. Sie nutzt IAM-Geschäftsservices und verarbeitet Informationen von IAM-Dienstanbietern für den Schutz seiner Ressourcen. Sie braucht zur Beurteilung der Berechtigung eines Ressourcenzugriffs nähere Informationen zu einem Subjekt.

Synonyme: Informationsbezüger, Informationskonsument, Lösungsanbieter, Service Provider

2.112 Replizierendes IAM-System

Ein replizierendes IAM-System verwaltet Benutzerdaten (E-Identities und Attribute) zentral an einem Standort. Während der Etablierung eines replizierenden IAM-Systems werden die Daten, die für die Erstellung einer E-Identity aggregiert (von mehreren Quellen kopiert und persistiert) und harmonisiert. Während des Betriebes des replizierenden IAM-Systems können die Daten von den Quellen periodisch aktualisiert werden.

Die Datenquellen sind im Unterschied zu einem föderierten IAM-System (siehe 2.57 Föderiertes IAM-System) nicht eigenständig.

2.113 Ressource

Service oder Daten, auf welche ein Subjekt zugreifen kann, wenn es sich authentisiert hat und es auf der Basis der benötigten Attribute autorisiert wurde. Dies schliesst physische Ressourcen wie Gebäude und Anlagen, deren Benutzung über IT-Systeme gesteuert wird, ein.

2.114 Ressourcen-Verantwortlicher

Verantwortliche Stelle für die von der Relying Party verwalteten Ressourcen (z.B.: Anwendungsverantwortlicher, Serviceverantwortlicher, Dateninhaber).

2.115 Role based Access Control (RBAC)

Verfahren zur Zugriffssteuerung und -kontrolle auf Dateien oder Dienste.

Bei der rollenbasierten Zugriffskontrolle werden Benutzern oder Gruppen von Benutzern eine oder mehrere Rollen zugeordnet. Eine Rolle enthält eine Menge von Berechtigungen (Permissions), die die erlaubten Operationen auf einer Ressource beschreiben. vgl. 2.7 Attribute-Based Access Control (ABAC)

Synonym: Rollenbasierte Zugriffskontrolle

2.116 Rolle

a) Organisation, Subjekt: Bestimmte Anzahl von Funktionen, die in einer Organisation ausgeführt werden. Einem Subjekt können eine oder mehrere Rollen zugeteilt werden.

b) E-Identity: Attribute, die die Rolle/Funktionen des Subjekts repräsentieren

c) System, Entität: Aufgabe und Zweck einer Entität in einer Föderation. Einer Entität können eine oder mehrere Rollen zugeteilt werden.

Synonym: Role

2.117 SAML 2.0 Web Browser SSO Profile

Profile fassen spezielle Anwendungsfälle von SAML zusammen. Das SAML 2.0 Web Browser SSO (single-sign-on) Profil [14] beschreibt webbasierte Authentisierungsszenarien, inkl. Identity Federation, für Browser.

2.118 SAML Protokoll

OASIS hat mit der Einführung von SAML nicht nur das SAML Token, sondern auch ein Protokoll und Bindings definiert, welche die Übertragung der Token spezifizieren. SAML unterstützt unter anderem HTTP-POST und HTTP-Redirect als Request-Response Schema. Nebst SAML gibt es auch andere Protokolle, welche SAML Token unterstützen. Zwei Beispiele dafür sind WS-Federation und WS-Trust.

2.119 SAML Token

Ein SAML Token enthält bestätigte Identitätsinformationen eines Subjekts in standardisierter Form. Kernpunkt eines SAML Tokens ist die Assertion. Diese beschreibt, zu wem das Token gehört, wie lange es gültig ist, wer es ausgestellt hat und dann die Identitätsinformationen des Subjekts und allfällige Attribute, welche an dieses geknüpft sind.

2.120 Security Assertion Markup Language (SAML)

SAML (Security Assertion Markup Language) erlaubt es, Informationen über Authentifizierungs- und Attributinformationen zwecks Autorisierung standardisiert zwischen mehreren Teilnehmern auszutauschen. Der SAML-Standard [14] beschreibt die Syntax und Regeln zum Anfordern, Erstellen und Austauschen von SAML-Assertions.

2.121 Security Token

Ein Datenpaket, welches verwendet werden kann, um den Zugriff auf eine Ressource zu autorisieren.

Ein Security Token enthält bestätigte Identitätsinformationen eines Subjekts in standardisier-

ter Form (Authentication Statement, Authentication Assertion). Eine Relying Party verifiziert und validiert diese Informationen, um daraus einen Zugangsentscheid abzuleiten.

2.122 Security Token Service (STS)

Security Token Service ist ein Webservice, welcher Security Tokens gemäss WS-Security Spezifikation [15] ausstellt.

2.123 Service Level Agreement (SLA)

Bezeichnet einen Vertrag zwischen Auftraggeber und Dienstleister für wiederkehrende Dienstleistungen.

2.124 Senderbaustein

Der Sender-Baustein realisiert eine standardisierte STIAM-Schnittstelle zur Anbindung einer Attribut-Autorität, welche die STIAM-Protokolle nicht direkt unterstützt, an den STIAM-Hub (vgl. 2.132 STIAM-Komponente Abbildung 3: STIAM-Komponenten).

2.125 Single Factor Cryptographic Devices

Ein single-factor cryptographic device ist ein physisches Gerät, welches kryptographische Berechnungen anhand einer dem Gerät gegebenen Eingabe durchführt. Das Gerät benötigt dazu keine Aktivierung über einen zweiten Authentifizierungsfaktor. Das Gerät benutzt zur Generierung des Ausgabewerts in ihm gespeicherte symmetrische oder asymmetrische Schlüssel. Die Authentifizierung wird durch den Besitznachweis des Gerätes vollbracht.

Beispiel: Yubikey U2F

Detaillierte Anforderungen sind in den folgenden Quellen beschrieben:
Siehe auch NIST SP 800-63B [10], Kapitel 5.1.6.

Synonym: Einfaktor Verschlüsselungsgeräte

2.126 STIAM Certificate Authority (STIAM-CA)

Ein STIAM-CA ist ein CA, der von der STIAM-Community akzeptiert wird.

2.127 STIAM Identity und Attribute Bus

Vermittelt Authentisierungs- und Attributanfragen zwischen Subjekt, RP, AuthnA und AA.

Nimmt die SAML-Requests der STIAM-Empfänger entgegen und leitet sie an die korrekte AuthnA und AA weiter. Danach nimmt er die Responses der STIAM-Sender entgegen und sendet die Informationen als aggregierte SAML-Response an die korrekte RP zurück.

2.128 STIAM-Community

Die STIAM-Community bilden alle Teilnehmer, die mit einer STIAM-Plattform interagieren und die einheitliche Spezifikation (vgl. 2.102 Policy) berücksichtigen.

2.129 STIAM-Empfänger

Kommunikationsmodul, das die standardisierte SAML-Kommunikation zwischen der RP und dem STIAM-Hub realisiert.

Der STIAM-Empfänger nutzt die Dienste des STIAM-Hubs, um einen Benutzer authentifizieren zu lassen und weitere Informationen über diesen zu beziehen, die dann zur Zugangssteuerung verwendet werden können. Der STIAM-Empfänger definiert, wie der Benutzer authentifiziert werden soll und welche Attribute in welcher Qualität notwendig sind, um Zugang auf eine seiner geschützten Ressourcen zu erlauben. Der STIAM-Empfänger erhält vom STIAM-Hub die geforderten Informationen in Form einer Authentifizierungs- und/oder Attributbestätigung.

2.130 STIAM-Hub

Der STIAM-Hub als Kernstück der SuisseTrustIAM-Plattform hat zwei Funktionen. Erstens bietet er zur Definitionszeit die Trust- und E-Identity-Geschäftsservices an, indem sich Benutzer und Organisationen auf dem STIAM-Hub registrieren können und zweitens agiert er als Vermittler (Broker) zwischen den Entitäten zur Laufzeit. Die administrativen Aufgaben auf dem STIAM-Hub können grob in folgende Prozesse und Funktionen aufgeteilt werden:

User Management: Benutzer können auf dem STIAM-Hub einen User-Account eröffnen und diesen verwalten. Alternativ ist es auch möglich, dass ein System Administrator einer Organisation User-Accounts für einen (oder mehrere) Benutzer bzw. Maschinen erstellen kann.

Organisation Management: Eine Organisation wird vom SuisseTrustIAM Betreiber initial in der Datenbasis eröffnet. Ein Mitarbeitender der Organisation (in der Rolle eines Organisationsverantwortlichen) wird dabei ermächtigt, bestimmte Eigenschaften der Organisation zu administrieren und zusätzliche Systemadministratoren zu erstellen und zu ermächtigen. Damit können administrative Aufgaben der Organisation aufgetrennt und delegiert werden.

Komponenten Management: Ziel der zentralen Administration auf dem STIAM-Hub ist die einfache und selbstständige Verwaltung der STIAM-Komponenten durch deren Systemverantwortlichen. Dieser kann selbstständig einzelne Komponenten zu SuisseTrustIAM hinzufügen bzw. verwalten. Für diese Komponenten müssen bestimmte Parameter, welche für ihre Rolle innerhalb der STIAM-Plattform notwendig sind, erfasst und konfiguriert werden.

Attribut Management: Der SuisseTrustIAM Betreiber unterhält eine Liste von Attributen, welche in der SuisseTrustIAM-Community verwendet werden können.

2.131 STIAM-IdP

Interner IdP einer STIAM-Plattform. Dient dem Registrieren und Initialisieren von STIAM Accounts und liefert qualitativ minimale Authentifikation der Subjekte.

Ein Identity Provider hat in STIAM die Funktion, ein Subjekt zu authentifizieren. Ein STIAM-IdP implementiert eine standardisierte STIAM-Schnittstelle zum STIAM-Hub (vgl. 2.132 STIAM-Komponente Abbildung 3).

2.132 STIAM-Komponente

Zu den STIAM-Komponenten gehören STIAM-Sender (Attribut-Autorität), STIAM-Empfänger (Relying Party), STIAM-IdPs, der STIAM-Hub und STIAM-CSPs. Die STIAM-Komponenten besitzen eine standardisierte Schnittstelle, die es ihnen erlaubt, miteinander zu kommunizieren und sich gegenseitig zu vertrauen.

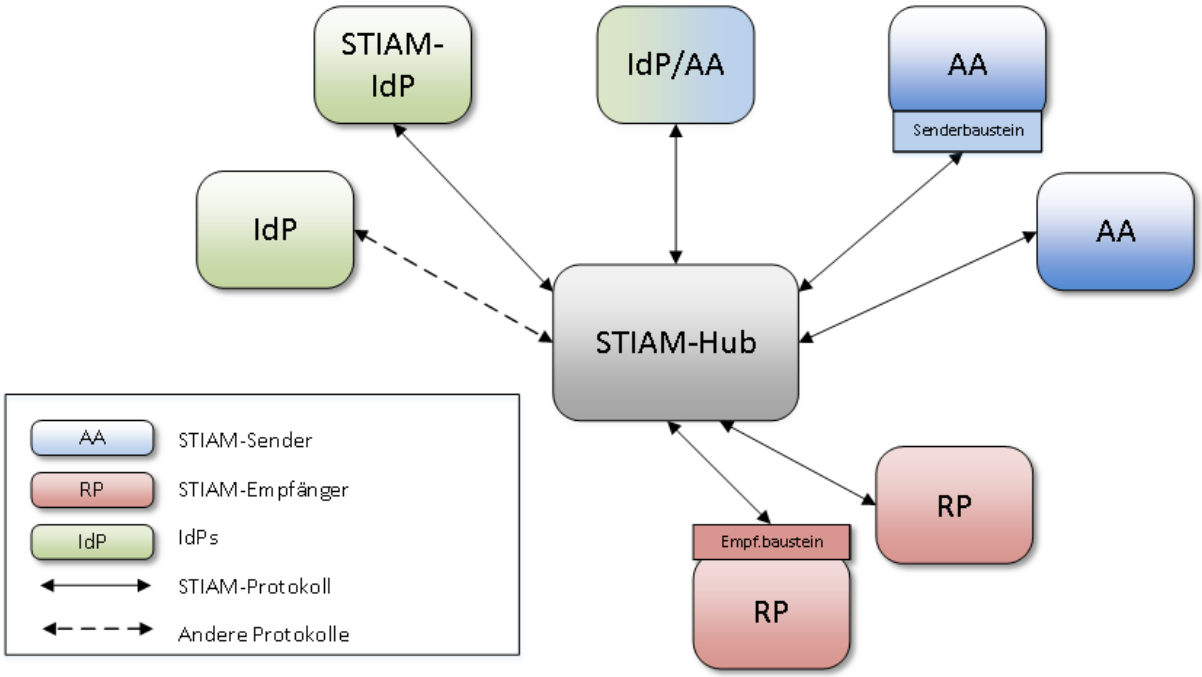


Abbildung 3: STIAM-Komponenten

2.133 STIAM-Metadata Repository (STIAM-MDR)

Zentraler Auskunftsdienst der STIAM-Plattform, verwaltet und publiziert die Metadaten für die STIAM-Community.

2.134 STIAM-Plattform

Die STIAM-Plattform umfasst den STIAM-Hub sowie alle zusätzlichen STIAM-spezifischen Komponenten (STIAM-Sender, STIAM-Empfänger, STIAM-CSP) die den Betrieb der funktionalen Lösung ermöglichen.

2.135 STIAM-RLM (Reporting-Logging-Monitoring)

Zur Gewährleistung der Nachvollziehbarkeit und Nachweisbarkeit werden Zugriffe auf Ressourcen gespeichert. Mit dem STIAM-RLM sollen analog dazu alle Vorgänge, die vom STIAM-Hub vermittelt werden, geloggt und überwacht werden können.

2.136 STIAM-Sender

Kommunikationsmodul, das die standardisierte SAML-Kommunikation zwischen der AA und

dem STIAM-Hub realisiert.

Der STIAM-Sender ist eine Attribut-Autorität (in der Regel Verzeichnisse oder Register), die Attribute für die STIAM-Community in standardisierter Form bereitstellt. Der STIAM-Sender hat ein standardisiertes Interface zum STIAM-Hub (vgl. 2.132 STIAM-Komponente Abbildung 3).

2.137 Subjekt

Ein Subjekt ist eine natürliche Person, eine Organisation (juristische Person), ein Service oder ein Ding, das auf eine Ressource zugreift oder zugreifen möchte. Ein Subjekt wird durch E-Identities repräsentiert.

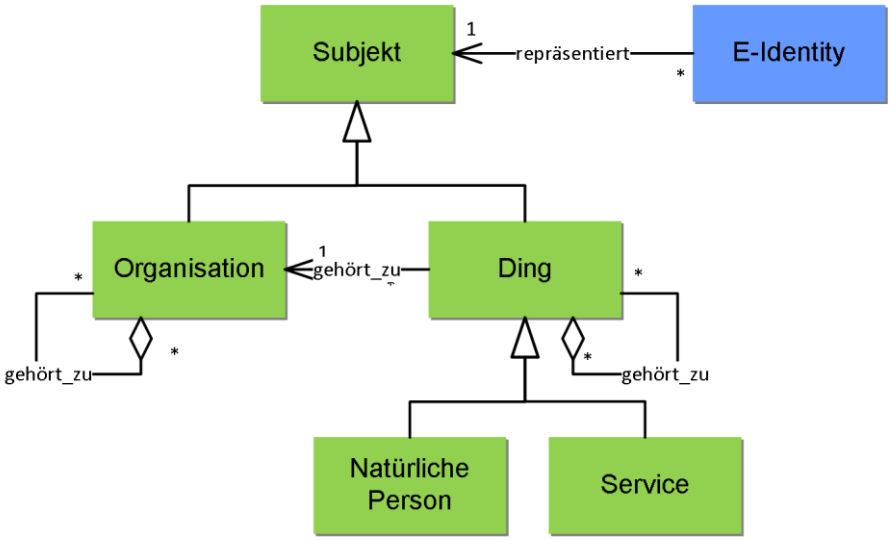


Abbildung 4: Definition Subjekt

Ein Abonnent (engl. Subscriber, siehe NIST 800-63-3A [16]) ist ein Subjekt, welches nach erfolgreich abgeschlossenem Registrationsprozess (Prozess Subjekt registrieren) ein Authentifizierungsmittel von einer CSP erhalten hat. Damit wird das Subjekt zu einem autorisierten Teilnehmer in der Identity Federation Community.

Ein Antragsteller (engl. Applicant, siehe NIST 800-63-3A [16]), ist ein Subjekt, das in die Identity Federation Community aufgenommen werden möchte und dazu den Prozess Subjekt registrieren durchläuft. Wurde dieser erfolgreich abgeschlossen, wird aus dem Antragsteller ein Abonnent.

Ein Überbringer (engl. Bearer) ist ein Subjekt, das eine vom IdP ausgestellte Authentifizierungsbestätigung an die RP übergibt.

2.138 Trust Service

Der Trust Service pflegt die akzeptierten, vertrauenswürdigen IAM-Dienstanbieter.

2.139 Trusted Third Party

Vertrauenswürdige Instanz, z.B. zur Verwaltung von öffentlichen Schlüsseln oder Zertifikaten.

2.140 UID-Einheit

UID-Einheiten sind nach Art. 3.c des Bundesgesetzes über die Unternehmens-Identifikationsnummer [17] festgelegt.

Bei UID-Einheiten handelt es sich um alle Unternehmen und Institutionen, die eine UID erhalten. Im UID-System ist der Unternehmensbegriff weit gefasst. Unter UID-Einheit versteht man somit nicht nur alle in der Schweiz tätigen Unternehmen im eigentlichen Sinn, sondern alle «Kundinnen und Kunden der öffentlichen Verwaltung», die Charakteristiken eines Unternehmens aufweisen oder die zu rechtlichen, administrativen oder statistischen Zwecken identifiziert werden.

Weitere Informationen zu der Unternehmens-Identifikationsnummer sind beim Bundesamt für Statistik vorhanden[4].

2.141 Verlässliche Quelle

Eine verlässliche Quelle ist eine beliebige Informationsquelle, welche bezogen auf eine konkrete Situation als vertrauenswürdig betrachtet wird.

eIDAS 2015/1502: „Verlässliche Quelle“ ist eine beliebige Informationsquelle, die auf verlässliche Weise präzise Daten, Informationen und/oder Beweismittel bereitstellt, die zum Identitätsnachweis verwendet werden können.

Verlässliche Quellen können viele verschiedene Formen haben, z.B. Register, Urkunden, Stellen usw.

2.142 Vermittler

Ein Vermittler bietet gemeinsame Dienste, wie Metadaten, Discovery oder Identity Linking, für alle anderen Stakeholder in einer Identity Föderation an. Siehe auch 2.28 Broker Service, 2.130 STIAM-Hub

Synonym: Broker

2.143 Vertrauen

Formell meist im SLA definierte Vertrauensbeziehung zwischen verantwortlichen Stellen. z.B. die formelle Beschreibung der Kriterien, die erfüllt sein müssen, damit sich zwei Organisationen, Entitäten, Domänen etc. gegenseitig vertrauen.

Synonym: Trust

2.144 Vertrauensstufe

Die Vertrauensstufe besagt mit welcher Qualität ein Subjekt authentifiziert wurde. Anhand von 4 Teilmodellen (Vertrauensstufe der Authentifizierung, Vertrauensstufen der Registrierung, Vertrauensstufen der Steuerung und Vertrauensstufen der Föderierung) wird die Ge-

[4] https://www.bfs.admin.ch/bfs/de/home/register/unternehmensregister/unternehmens-identifikationsnummer/uid-einheiten-unternehmen.html

samt-Vertrauensstufe bestimmt.

Synonym: Vertrauensniveau

2.145 Verwaltung

Verwaltung bezeichnet ein Gemeinwesen (Ämter und Behörden, allenfalls mit solchen Aufgaben beauftragte Private), welches gesetzlich übertragene Staatsaufgaben besorgt. Der Begriff Verwaltung ist ein organisatorischer Begriff, der ausserhalb der juristischen Definition von natürlicher und juristischer Person steht.

2.146 Verzeichnis

Systematische Sammlung von Informationen mit gemeinsamen Merkmalen.

2.147 Widerruf

Beim Zertifikatswiderruf handelt es sich um eine Erklärung der Ungültigkeit eines digitalen Zertifikats. Analog können auch elektronische Identifizierungsmittel widerrufen werden.

Synonyme: Revokation, Revocation, Sperrung

2.148 WS-Federation

WS-Federation in der aktuellen Version 1.2 [15] ist ebenfalls Teil der WS-* Spezifikation und erweitert WS-Trust mit der Möglichkeit, Security Tokens auch über unterschiedliche Domains auszutauschen, indem der Standard mehrere Identity Provider unterstützt. Bei WS-Federation kann das SAML-Tokenformat als Security Token verwendet werden.

2.149 WS-Trust

Der von OASIS spezifizierte Web Service Trust (WS-Trust) [15] in der aktuellen Version 1.4 ist Teil der WS-* Spezifikation, welche ein Framework für den sicheren Austausch von Web Service Nachrichten bereitstellt. Bei WS-Trust handelt es sich um einen Standard, der die Interoperabilität von Sicherheits-Token durch Definition eines Protokolls für Anforderungen und Antworten unterstützt. Dieses Protokoll ermöglicht einem Consumer (z.B. ein Web-Service-Client), den Austausch eines bestimmten Sicherheitstokens von einem anerkannten Aussteller, dem Security Token Service (STS), anzufordern und einer Relying Party zu übergeben. Bei WS-Trust kann das SAML-Tokenformat als Security Token verwendet werden.

2.150 Zugang Service

Der Service überprüft die Einhaltung der Zugangsregeln und erlaubt dem Subjekt den Zugang, wenn die entsprechenden Regeln erfüllt sind.

Synonym: Access Service

2.151 Zugangsregel

Ressourcenverantwortliche definieren die Zugangsregeln für ihre E-Ressourcen. Die Zugangsregeln definieren die Bedingungen, unter denen ein Subjekt Zugang zu einer Ressource erhält (Grobautorisierung), z.B. nach erfolgreicher Authentifizierung und Bestätigung bestimmter Attribute.

2.152 Zugangsregel Service

Der Service verwaltet die Regeln für den Zugang zu einer Ressource. Die Regeln sind auf der Basis von Authentisierung oder Attributen definiert.

2.153 Zugriff

Interaktion mit einer Entität um eine oder mehrere ihrer Ressourcen zu manipulieren und oder zu nutzen [3].

Zur Gewährleistung der Nachvollziehbarkeit und Nachweisbarkeit werden Zugriffe gespeichert.

Synonym: Access

2.154 Zugriffskontrolle

Überwachung und Steuerung des Zugriffs auf Ressourcen. Das Ziel ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen.

Synonym: Access Control

2.155 Zugriffsrecht

Ressourcenverantwortliche definieren die Zugriffsrechte für ihre E-Ressourcen. Die Zugriffsrechte definieren die Bedingungen unter denen ein Subjekt auf die verschiedenen Funktionalitäten einer Ressource nutzen darf (Feinautorisierung), z.B. nach erfolgreicher Authentifizierung und Bestätigung bestimmter Attribute.

2.156 Zugriffsrecht Service

Der Service verwaltet die Rechte für die Nutzung einer E-Ressource. Die Rechte sind auf der Basis von Authentifizierung, Attributen oder eigenen Modellen (Gruppen, Rollen, Einzelberechtigungen) definiert.

3 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellen oder welche **eCH** referenzieren, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der

Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

4 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende, sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Anhang A – Referenzen & Bibliographie

[1] Schweizerische Eidgenossenschaft, “Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES),” 2016 [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20131913/index.html

[2] N. Klingenstein, “Attribute aggregation and federated identity,” *SAINT - 2007 Int. Symp. Appl. Internet - Work. SAINT-W*, 2007.

[3] S. Cantor, J. Hodges, F. Hirsch, R. Philpott, R. S. a Security, J. Hughes, A. Origin, H. Lockhart, B. E. a Systems, M. Beach, R. Metz, B. A. Hamilton, R. Randall, T. Wisniewski, I. Reid, P. Austel, R. L. B. Morgan, P. C. Davis, J. Kemp, P. Madsen, A. Anderson, and S. Microsystems, “Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0,” *Oasis Stand.*, 2005 [Online]. Available: https://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf

[4] N. Ragouzis, J. Hughes, R. Philpott, E. Maler, P. Madsen, and T. Scavo, “Security Assertion Markup Language (SAML) V2.0 Technical Overview (OASIS),” 2007 [Online]. Available: https://www.oasis-open.org/committees/security/docs/draft-sstc-baker-saml-arch-00.pdf

[5] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, and C. Mortimore, “OpenID Connect Core 1.0 incorporating errata set 1,” 2014 [Online]. Available: http://openid.net/specs/openid-connect-core-1_0.html

[6] J. L. F. Paul A. Grassi, “DRAFT NIST Special Publication 800-63-3,” 2017 [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63-3.html. [Accessed: 22-Jun-2017]

[7] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, W. E. Burr, D. F. Dodson, and R. A. Perlner, “NIST Special Publication 800-63-2 Electronic Authentication Guideline,” 2003 [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[8] NIST, “DRAFT Strength of Function for Authenticators - Biometrics.” [Online]. Available: https://pages.nist.gov/SOFA/SOFA.html. [Accessed: 03-Nov-2016]

[9] P. Editors, W. Fumy, M. De Soete, E. J. Humphreys, K. Naemura, and K. Rannenberg, “ITU-T Recommendation X . 1254 | International Standard ISO / IEC DIS 29115 Information technology — Security techniques — Entity authentication assurance framework,” 2011.

[10] J. P. R. Paul A. Grassi, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, James L. Fenton, “DRAFT NIST Special Publication 800-63B,” 2017 [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html. [Accessed: 22-Jun-2017]

[11] D. A. S. Europ, I. Parlamentder, R. A. T. D. E. R. Europ, and I. Union, “VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, (eIDAS),” 2015.

[12] E. D. Hardt, “The OAuth 2.0 Authorization Framework [RFC 6749],” 2012 [Online]. Available: https://tools.ietf.org/html/rfc6749

[13] M. Jones, J. Bradley, and N. Sakimuar, “JSON Web Token (JWT),” 2015 [Online]. Available: https://tools.ietf.org/pdf/rfc7519.pdf

[14] S. Cantor, J. Hodges, F. Hirsch, R. Philpott, R. S. a Security, J. Hughes, A. Origin, H.

Lockhart, B. E. a Systems, M. Beach, R. Metz, B. A. Hamilton, R. Randall, T. Wisniewski, I. Reid, P. Austel, R. L. B. Morgan, P. C. Davis, J. Kemp, P. Madsen, A. Anderson, and S. Microsystems, “Profiles for the OASIS Security Assertion Markup Language (SAML),” *Oasis Stand.*, 2005 [Online]. Available: https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[15] K. Lawrence, C. Kaler, A. Nadalin, M. Goodner, and M. Gudgin, “WS-Trust 1.4,” *Oasis Stand.*, no. April, 2012 [Online]. Available: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html

[16] J. L. F. Paul A. Grassi, Jamie M. Danker, William E. Burr, “DRAFT NIST Special Publication 800-63A,” 2017 [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63a.html. [Accessed: 22-Jun-2017]

[17] D. Bundesversammlung and D. S. Eidgenossenschaft, *Bundesgesetz über die Unternehmens-Identifikationsnummer (UIDG)*. 2011 [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20082601/index.html

Anhang B – Mitarbeit & Überprüfung

Gruoner Torsten	Bundesverwaltung – EFD – ISB
Hassenstein Gerhard	Berner Fachhochschule, TI
Heerkens Marc	Bundesverwaltung – EFD – ISB
Kunz Marc	Berner Fachhochschule, TI
Laube-Rosenpflanzer Annett	Berner Fachhochschule, TI
Müller Adrian	ID Cyber-Identity Ltd
Selzam Thomas	Berner Fachhochschule, FBW
Spichiger Andreas	Berner Fachhochschule, FBW
	eCH Fachgruppe IAM

Anhang C – Abkürzungen

CA	Credential Authority
CSP	Credential Service Provider
eIDAS	Verordnung (EU) Nr. 910/2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnen-markt
EU	Europäische Union
FIDO	Fast IDentity Online
HTTP	Hypertext Transfer Protocol

HW-MFA	Hardware Multifactor Authentication
IAM	Identity and Access Management
IdP	Identity Provider
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KDC	Kerberos Distribution Center
MFA	Mulit Factor Authentication
NIST	National Institute of Standards and Technology
nPA	neuer Personalausweis
OIDC	OpenID Connect
OTP	One-time Password
PIN	Persönliche Identifikaitonsnummer
RA	Register Authority / Registrierungsstelle
RP	Relaying Party
SAML	Security Assertion Markup Language
SFA	Single Factor Authentication
SMS	Short Message Service
SSO	Single Sign-on
STORK	Secure idenTity acrOss boRders linKed
TGT	Ticket Granting Ticket
TSP	Trust Service Provider
UID	Unique identifier
URL	Uniform Resource Locator
ZGB	Schweizerisches Zivilgesetzbuch

Anhang E – Abbildungsverzeichnis

Anhang F – Tabellenverzeichnis